



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR    | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|-------------------------|---------------------|------------------|
| 09/734,105      | 12/11/2000  | David Carroll Challener | RPS920000074US1     | 3775             |

7590 05/06/2004

BRACEWELL & PATTERSON, L.L.P.  
INTELLECTUAL PROPERTY LAW  
P. O. BOX 969  
AUSTIN,, TX 78767-0969

|          |
|----------|
| EXAMINER |
|----------|

SHERKAT, AREZOO

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2131

DATE MAILED: 05/06/2004

7

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/734,105

Applicant(s)

CHALLENGER ET AL.

Examiner

Arezoo Sherkat

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 11 December 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 December 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

Claims 1-19 have been presented for examination.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-5, 10-13, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mamata, (U.S. Patent No. 6,067,589 and Mamata hereinafter), in view of Angelo et al., (U.S. Patent No. 5,748,888 and Angelo hereinafter).

Regarding claim 1, Mamata discloses a method for securing access to a keyboard driver in a host computer, wherein said host computer includes a host processor that manages communication between said keyboard driver and a keyboard attached to said host computer, said method comprising:

receiving a packet on a bus that provides a communication medium between said keyboard and said host computer (Col. 7, lines 7-67 and Col. 8, lines 1-34).

Mamata does not expressly disclose setting an input secure bit only in response to determining that said packet originated from said keyboard.

However, Angelo discloses

setting an input secure bit only in response to determining that said packet originated from said keyboard, wherein said set input secure bit is subsequently utilized to access said keyboard driver from said host processor (Col. 7, lines 14-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Mamata with the teachings of Angelo because it would allow to include setting an input secure bit only in response to determining that said packet originated from said keyboard with the motivation to provide a secure keyboard communications channel and overcome the problem of keyboard sniffing (Angelo, Col. 2, lines 1-50).

Regarding claim 2, Mamata does not expressly disclose further comprising reading said input secure bit to determine whether or not said keyboard driver may be accessed by said host processor.

However, Angelo discloses further comprising reading said input secure bit to determine whether or not said keyboard driver may be accessed by said host processor (Col. 7, lines 35-47).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Mamata with the teachings of Angelo because it would allow to include setting an input secure bit only in response to determining that said packet originated from said keyboard with the motivation to provide a secure keyboard communications channel and overcome the problem of keyboard sniffing (Angelo, Col. 2, lines 1-50).

Regarding claim 3, Mamata does not expressly disclose setting an input secure bit only in response to determining that said packet originated from said keyboard.

However, Angelo discloses further comprising:

detecting if said input secure bit has been read, and in response to detecting that said input secure bit has been read, clearing said input secure bit (Col. 7, lines 47-67 and Col. 8, lines 1-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Mamata with the teachings of Angelo because it would allow to include setting an input secure bit only in response to determining that said packet originated from said keyboard with the motivation to provide a secure keyboard communications channel and overcome the problem of keyboard sniffing (Angelo, Col. 2, lines 1-50).

Regarding claim 4, Mamata discloses further comprising scanning packets on said bus during operation of said host processor (i.e., the SM-BIOS reads and interprets the packets of USB Keyboard from the USB Host Controller to transform it into data corresponding to PS/2 keyboard ...)(Col. 7, lines 7-67 and Col. 8, lines 1-34).

Regarding claim 5, Mamata discloses wherein said keyboard includes a keyboard controller for receiving and responding to keystrokes from said keyboard, and

wherein said method further comprises determining whether said packet originated from said keyboard controller (Col. 1, lines 35-55).

Regarding claim 10, Mamata discloses a system for securing access to a keyboard driver in a host computer, wherein said host computer includes a host processor that manages communication between said keyboard driver and a keyboard attached to said host computer, said system comprising:

processing means for receiving a packet on a bus (i.e., USB Host Controller) that connects said keyboard to said host processor (i.e., reception of data from USB keyboard), and processing means for determining whether said packet originated from said keyboard (i.e., the SM-BIOS reads and interprets the packets of USB Keyboard from the USB Host Controller to transform it into data corresponding to PS/2 keyboard ...)(Col. 7, lines 7-67 and Col. 8, lines 1-34).

Mamata does not expressly disclose setting an input secure bit only in response to determining that said packet originated from said keyboard.

However, Angelo discloses

processing means responsive to determining that said packet originated from said keyboard for setting an input secure bit that is read by said host processor to selectively provide access to said keyboard driver in accordance with verification that said keyboard originated said packet (Col. 7, lines 14-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Mamata with the teachings

of Angelo because it would allow to include setting an input secure bit only in response to determining that said packet originated from said keyboard with the motivation to provide a secure keyboard communications channel and overcome the problem of keyboard sniffing (Angelo, Col. 2, lines 1-50).

Regarding claim 11, Mamata does not expressly disclose setting an input secure bit only in response to determining that said packet originated from said keyboard.

However, Angelo discloses further comprising:

processing means for detecting if said input secure bit has been read, and processing means responsive to detecting that said input secure bit has been read for clearing said input secure bit (Col. 7, lines 47-67 and Col. 8, lines 1-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Mamata with the teachings of Angelo because it would allow to include setting an input secure bit only in response to determining that said packet originated from said keyboard with the motivation to provide a secure keyboard communications channel and overcome the problem of keyboard sniffing (Angelo, Col. 2, lines 1-50).

Regarding claim 12, Mamata discloses further comprising processing means for scanning packets on said bus during operation of said host processor (i.e., the SM-BIOS reads and interprets the packets of USB Keyboard from the USB Host Controller

to transform it into data corresponding to PS/2 keyboard ...)(Col. 7, lines 7-67 and Col. 8, lines 1-34).

Regarding claim 13, Mamata discloses wherein said keyboard includes a keyboard controller for receiving and responding to keystrokes from said keyboard, and wherein said method further comprises determining whether said packet originated from said keyboard controller (Col. 1, lines 35-55).

Regarding claim 18, Mamata discloses a system for securing access to a keyboard driver in a host computer, wherein said host computer includes a host processor that manages communication between said keyboard driver and a keyboard, said system comprising:

a processor for analyzing traffic on a bus that connects said keyboard to said host computer, wherein said processor identifies packets that originate from said keyboard (Col. 5, lines 29-67 and Col. 6-7, lines 1-67 and Col. 8, lines 1-34).

Mamata does not expressly disclose setting an input secure bit only in response to determining that said packet originated from said keyboard.

However, Angelo discloses

an input secure bit that is set in response to said processor identifying a packet originating from said keyboard, wherein said input secure bit is utilized by said host processor to provide selective access to said keyboard driver (Col. 7, lines 14-67).



Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Mamata with the teachings of Angelo because it would allow to include setting an input secure bit only in response to determining that said packet originated from said keyboard with the motivation to provide a secure keyboard communications channel and overcome the problem of keyboard sniffing (Angelo, Col. 2, lines 1-50).

Claims 6-9, 14-17, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mamata, (U.S. Patent No. 6,067,589 and Mamata hereinafter) and Angelo et al., (U.S. Patent No. 5,748,888 and Angelo hereinafter), in view of Rawlins, (U.S. Patent No. 6,216,183 and Rawlins hereinafter).

Teachings of Mamata and Angelo have been discussed previously.

Regarding claim 6, the combined teaching of Mamata and Angelo does not expressly disclose further comprising determining a device address of said keyboard upon initialization of said keyboard with respect to said host computer.

However, Rawlins discloses further comprising determining a device address of said keyboard upon initialization of said keyboard with respect to said host computer (Col. 3, lines 26-67 and Col. 4, lines 1-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Mamata and Angelo with the teachings of Rawlins because it would allow to include determining a

device address of said keyboard upon initialization of said keyboard with respect to said host computer with the motivation to prevent unauthorized access of the system memory, especially in situations where the user-entered password is input to the system memory from a USB input device, such as a USB keyboard (Rawlins, Col. 1, lines 45-60).

Regarding claim 7, Mamata does not expressly disclose setting an input secure bit only in response to determining that said packet originated from said keyboard.

However, Angelo discloses an input secure bit that is set in response to said processor identifying a packet originating from said keyboard (Col. 7, lines 14-67).

The combined teaching of Mamata and Angelo does not expressly disclose wherein said step of determining a device address further comprises reading an address field of said data packet, determining whether or not said address field matches said keyboard device address.

However, Rawlins discloses wherein said step of determining a device address further comprises:

reading an address field of said data packet, determining whether or not said address field matches said keyboard device address (Col. 6, lines 17-65).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Mamata with the teachings of Angelo because it would allow to include setting an input secure bit only in response to determining that said packet originated from said keyboard with the motivation to

provide a secure keyboard communications channel and overcome the problem of keyboard sniffing (Angelo, Col. 2, lines 1-50), and to modify the combined teachings of Mamata and Angelo with the teachings of Rawlins because it would allow to include setting said input secure bit in response to determining that said address field matches said keyboard device address with the motivation to prevent unauthorized access of the system memory, especially in situations where the user-entered password is input to the system memory from a USB input device, such as a USB keyboard (Rawlins, Col. 1, lines 45-60).

Regarding claim 8, the combined teaching of Mamata and Angelo does not expressly disclose wherein said bus is a Universal Serial Bus (USB) such that said keyboard is identified by a USB device address, said step of determining a device address further comprising reading a USB address field of said packet.

However, Rawlins disclose wherein said bus is a Universal Serial Bus (USB) such that said keyboard is identified by a USB device address, said step of determining a device address further comprising reading a USB address field of said packet (Col. 6, lines 17-65).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Mamata and Angelo with the teachings of Rawlins because it would allow to include the step of determining a device address further comprising reading a USB address field of said packet with the motivation to prevent unauthorized access of the system memory,

especially in situations where the user-entered password is input to the system memory from a USB input device, such as a USB keyboard (Rawlins, Col. 1, lines 45-60).

Regarding claim 9, the combined teaching of Mamata and Angelo does not expressly disclose further comprising assigning a unique USB address to said keyboard.

However, Rawlins disclose further comprising assigning a unique USB address to said keyboard (Col. 2, lines 40-67 and Col. 3, lines 1-25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Mamata and Angelo with the teachings of Rawlins because it would allow to include assigning a unique USB address to said keyboard with the motivation to provide for securing against accessing sensitive information entered into memory by a universal serial bus ("USB") input device (Rawlins, Col. 1, lines 1-15).

Regarding claim 14, the combined teaching of Mamata and Angelo does not expressly disclose further comprising processing means for determining a device address of said keyboard upon initialization of said keyboard with respect to said host computer.

However, Rawlins discloses further comprising processing means (i.e., USB host controller within the bus interface Unit) for determining a device address of said

keyboard upon initialization of said keyboard with respect to said host computer (Col. 3, lines 26-67 and Col. 4, lines 1-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Mamata and Angelo with the teachings of Rawlins because it would allow to include determining a device address of said keyboard upon initialization of said keyboard with respect to said host computer with the motivation to prevent unauthorized access of the system memory, especially in situations where the user-entered password is input to the system memory from a USB input device, such as a USB keyboard (Rawlins, Col. 1, lines 45-60).

Regarding claim 15, Mamata does not expressly disclose setting an input secure bit only in response to determining that said packet originated from said keyboard.

However, Angelo discloses an input secure bit that is set in response to said processor identifying a packet originating from said keyboard (Col. 7, lines 14-67).

The combined teaching of Mamata and Angelo does not expressly disclose wherein processing means for reading an address field of said data packet, and processing means for determining whether or not said address field matches said keyboard device address.

However, Rawlins discloses wherein said step of determining a device address further comprises:

processing means (i.e., USB host controller) for reading an address field of said data packet, processing means for determining whether or not said address field matches said keyboard device address (Col. 6, lines 17-65).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Mamata with the teachings of Angelo because it would allow to include setting an input secure bit only in response to determining that said packet originated from said keyboard with the motivation to provide a secure keyboard communications channel and overcome the problem of keyboard sniffing (Angelo, Col. 2, lines 1-50), and to modify the combined teachings of Mamata and Angelo with the teachings of Rawlins because it would allow to include processing means for setting said input secure bit responsive to determining that said address field matches said keyboard device address with the motivation to prevent unauthorized access of the system memory, especially in situations where the user-entered password is input to the system memory from a USB input device, such as a USB keyboard (Rawlins, Col. 1, lines 45-60).

Regarding claim 16, the combined teaching of Mamata and Angelo does not expressly disclose wherein said bus is a Universal Serial Bus (USB) such that said keyboard is identified by a USB device address, said step of determining a device address further comprising processing means for reading a USB address field of said packet.

However, Rawlins disclose wherein said bus is a Universal Serial Bus (USB) such that said keyboard is identified by a USB device address, said step of determining a device address further comprising processing means (i.e., USB host controller) for reading a USB address field of said packet (Col. 6, lines 17-65).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Mamata and Angelo with the teachings of Rawlins because it would allow to include the step of determining a device address further comprising processing means for reading a USB address field of said packet with the motivation to prevent unauthorized access of the system memory, especially in situations where the user-entered password is input to the system memory from a USB input device, such as a USB keyboard (Rawlins, Col. 1, lines 45-60).

Regarding claim 17, the combined teaching of Mamata and Angelo does not expressly disclose further comprising processing means for of assigning a unique USB address to said keyboard.

However, Rawlins disclose further comprising processing means (i.e., USB host controller) for of assigning a unique USB address to said keyboard (Col. 2, lines 40-67 and Col. 3, lines 1-25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Mamata and Angelo with the teachings of Rawlins because it would allow to include assigning a

unique USB address to said keyboard with the motivation to provide for securing against accessing sensitive information entered into memory by a universal serial bus ("USB") input device (Rawlins, Col. 1, lines 1-15).

Regarding claim 19, Mamata discloses wherein said host computer is a Universal Serial Bus (USB) host that includes a USB host controller, and wherein said bus is a USB that provides USB connectivity between said keyboard and said host processor.

Mamata or Angelo does not expressly disclose that packets transferred on said USB conform to USB transfer protocol.

However, Rawlins discloses that packets transferred on said USB conform to USB transfer protocol (Col. 6, lines 17-32).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Mamata and Angelo with the teachings of Rawlins because it would allow to include packets transferred on said USB conform to USB transfer protocol with the motivation to provide useful functionality not only when connecting to existing bi-directional serial lines, but also as an overall expansion port to numerous hardware resources, such as keyboards, mice, etc (Rawlins, Col. 1, lines 60-67).

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:




Garney et al., (U.S. Patent No. 5,890,015),  
Miller, (U.S. Patent No. 6,629,793),  
Anderson et al., (U.S. Publication No. 2003/0217123), and  
Dickens, (U.S. Publication No. 2003/0188049).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (703) 305-8749. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Arezoo Sherkat  
Patent Examiner  
Technology Center 2100  
May 3, 2004

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100